Elementi essenziali e gestione della sicurezza informatica per il settore energetico

CSP001_C_E

PRESENTAZIONE DI:
ANTONIO MUÑOZ
UNIVERSITÀ DI MALAGA, SPAGNA

Ringraziamenti

- *Cofinanziato dall'Unione Europea. Le opinioni e i pareri espressi sono tuttavia esclusivamente quelli dell'autore/degli autori e non riflettono necessariamente quelli dell'Unione Europea o dell'HADEA. Né l'Unione Europea né l'autorità che ha concesso il finanziamento possono essere ritenute responsabili per essi.*
- *Accordo di progetto n. 101083594*

Argomento 5: Sicurezza Progettazione e implementazione sicura per i sistemi energetici

Panoramica

- Progettazione e implementazione di architetture di rete sicure per i sistemi energetici
- Architettura di rete sicura nel settore energetico, compresi i sistemi SCADA, le reti intelligenti e altre risorse energetiche critiche
- Utilizzo della segmentazione di rete per isolare i sistemi critici e ridurre l'impatto degli attacchi informatici
- Configurazione di firewall e sistemi di controllo degli accessi per proteggere le reti energetiche e limitare gli accessi non autorizzati
- Implementare sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS) per monitorare e proteggere le reti
- Impiego di VPN per un accesso remoto sicuro ai sistemi energetici e ai dati sensibili

Antonio Muñoz, Università di Malaga, Spagna

Argomento 5: Sicurezza Progettazione architettonica e implementazione per sistemi energetici

Panoramica

- **Progettazione e implementazione di architetture di rete sicure per sistemi energetici**
- Architettura di rete sicura nel settore energetico, compresi i sistemi SCADA, le reti intelligenti e altre risorse energetiche critiche
- Utilizzo della segmentazione di rete per isolare i sistemi critici e ridurre l'impatto degli attacchi informatici
- Configurazione di firewall e sistemi di controllo degli accessi per proteggere le reti energetiche e limitare gli accessi non autorizzati
- Implementare sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS) per monitorare e proteggere le reti
- Impiego di VPN per un accesso remoto sicuro ai sistemi energetici e ai dati sensibili

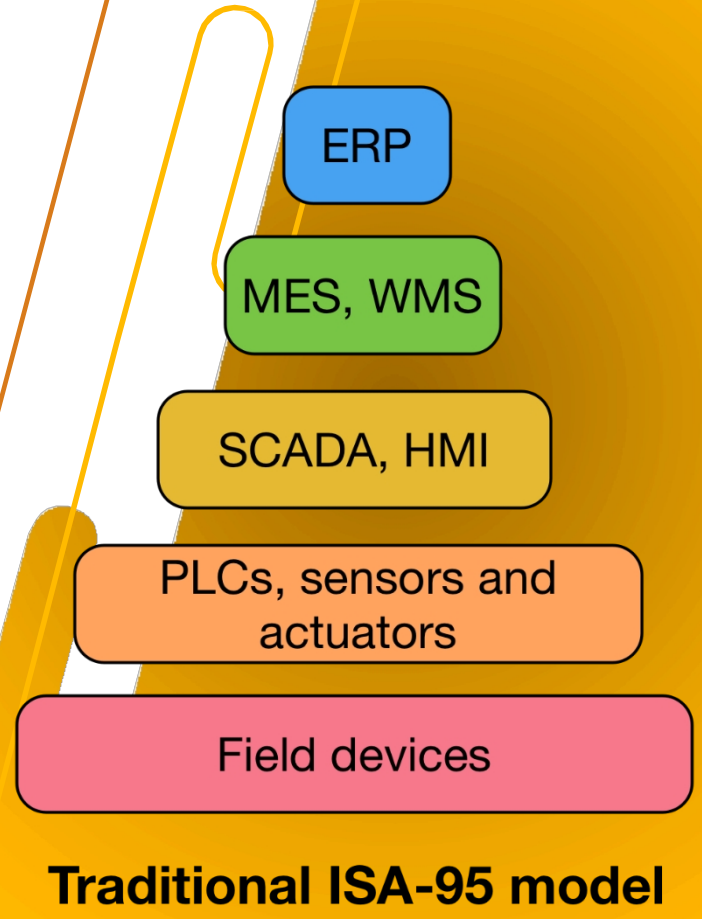
Antonio Muñoz, Università di Malaga, Spagna

Reti principali nei sistemi energetici

- Come indicato nell'argomento 2, **i sistemi SCADA (Supervisory Control and Data Acquisition)** fanno parte del processo di monitoraggio dei sistemi energetici
  - Sono responsabili della supervisione degli stati delle infrastrutture energetiche, dei loro processi operativi e dei loro componenti
  - I loro componenti principali si basano su elementi cyber-fisici con la capacità di:
    - Percepire gli stati contestuali dell'ambiente osservato
    - Elaborare queste informazioni e
    - agire di conseguenza nell'ambiente osservato

Reti principali nei sistemi energetici

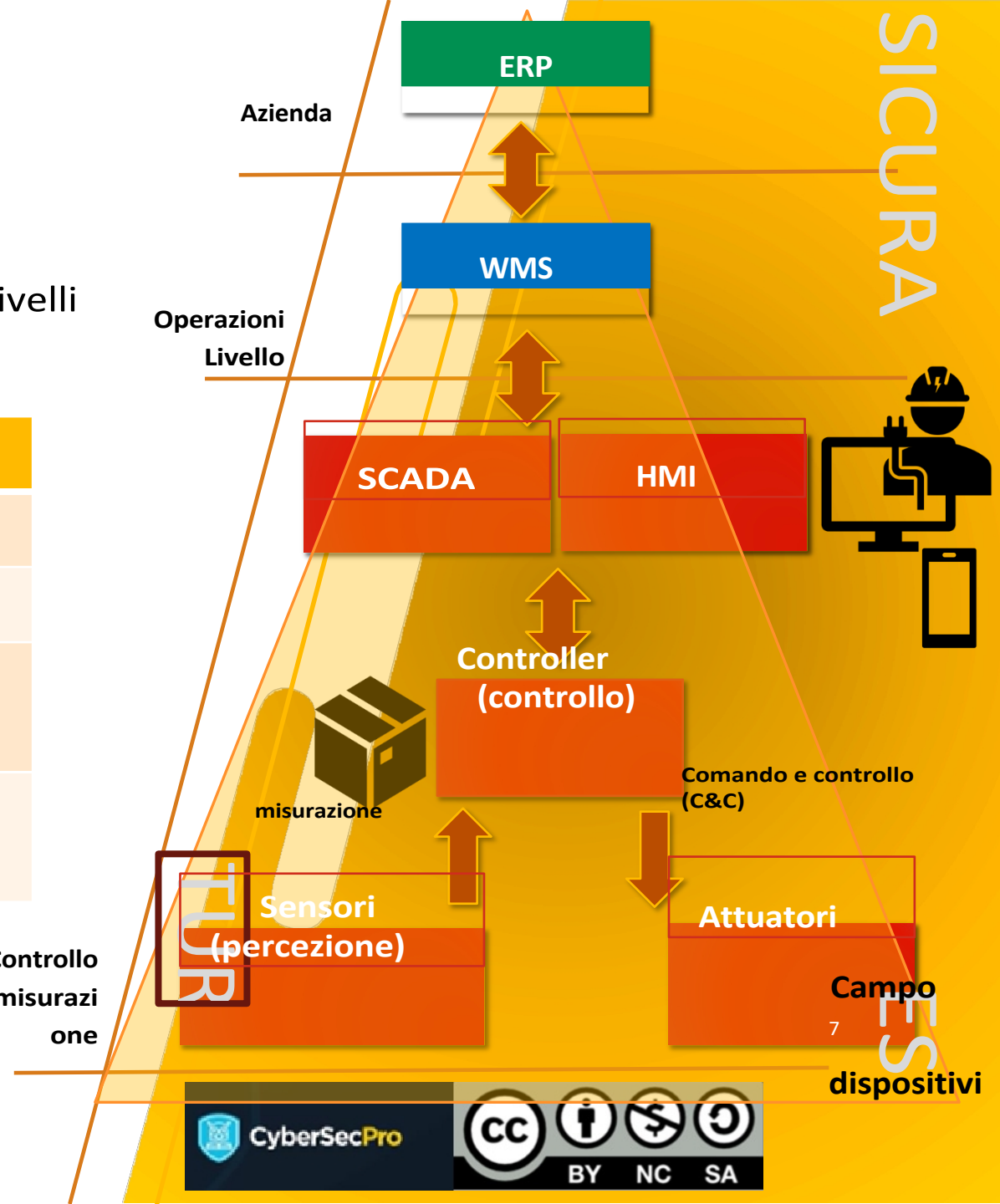
- Come indicato nell'argomento 2, **i sistemi SCADA (Supervisory Control and Data Acquisition)** fanno parte del processo di monitoraggio dei sistemi energetici
  - Sono incaricati di supervisionare gli stati delle infrastrutture energetiche, i loro processi operativi e i loro componenti
  - I loro componenti principali si basano su elementi cyber-fisici con la capacità di:
    - Percepire gli stati contestuali dell'ambiente osservato
    - Elaborare queste informazioni e
    - agire di conseguenza nell'ambiente osservato
- Questi sistemi seguono normalmente **strutture gerarchiche** in cui:
  - I dispositivi di campo si collegano ai controller
  - I controllori si collegano ai server SCADA e alle interfacce uomo-macchina (HMI)
  - I server SCADA si collegano ai sistemi di gestione del magazzino (WMS)
  - I WMS si collegano ai server di pianificazione delle risorse aziendali (ERP)



Principali reti nei sistemi energetici

- Questa gerarchia operativa è composta da una serie di livelli funzionali:

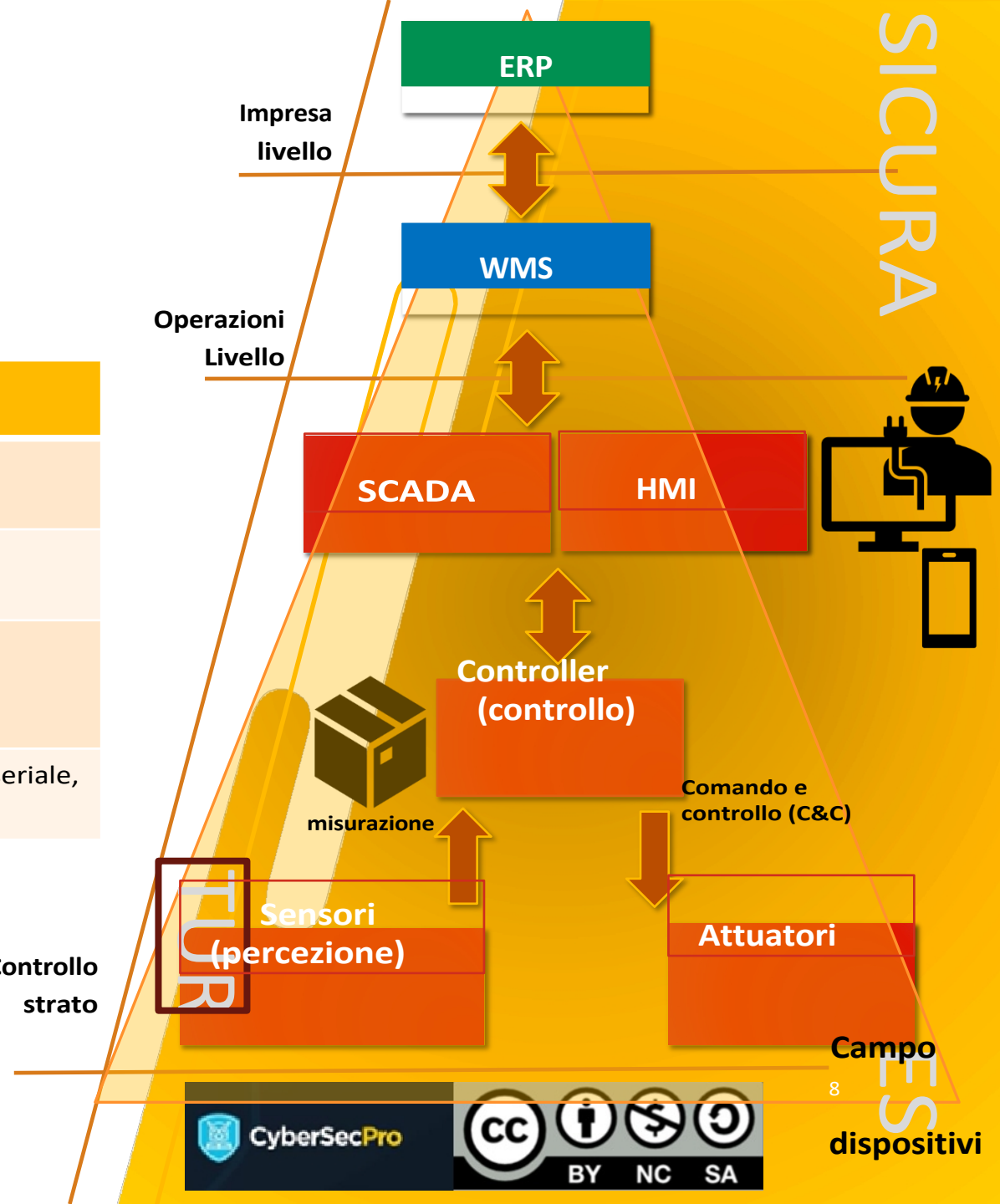
Livello funzionale	Componenti
Livello aziendale (ERP)	Server ERP
Livello operativo (WMS)	Server WMS
Livello di controllo	Server SCADA, HMI, controllori (PLC/RTU)
	Dispositivi di campo (sensori, attuatori)



Reti principali nei sistemi energetici

- Questa gerarchia operativa è composta da una serie di livelli funzionali:

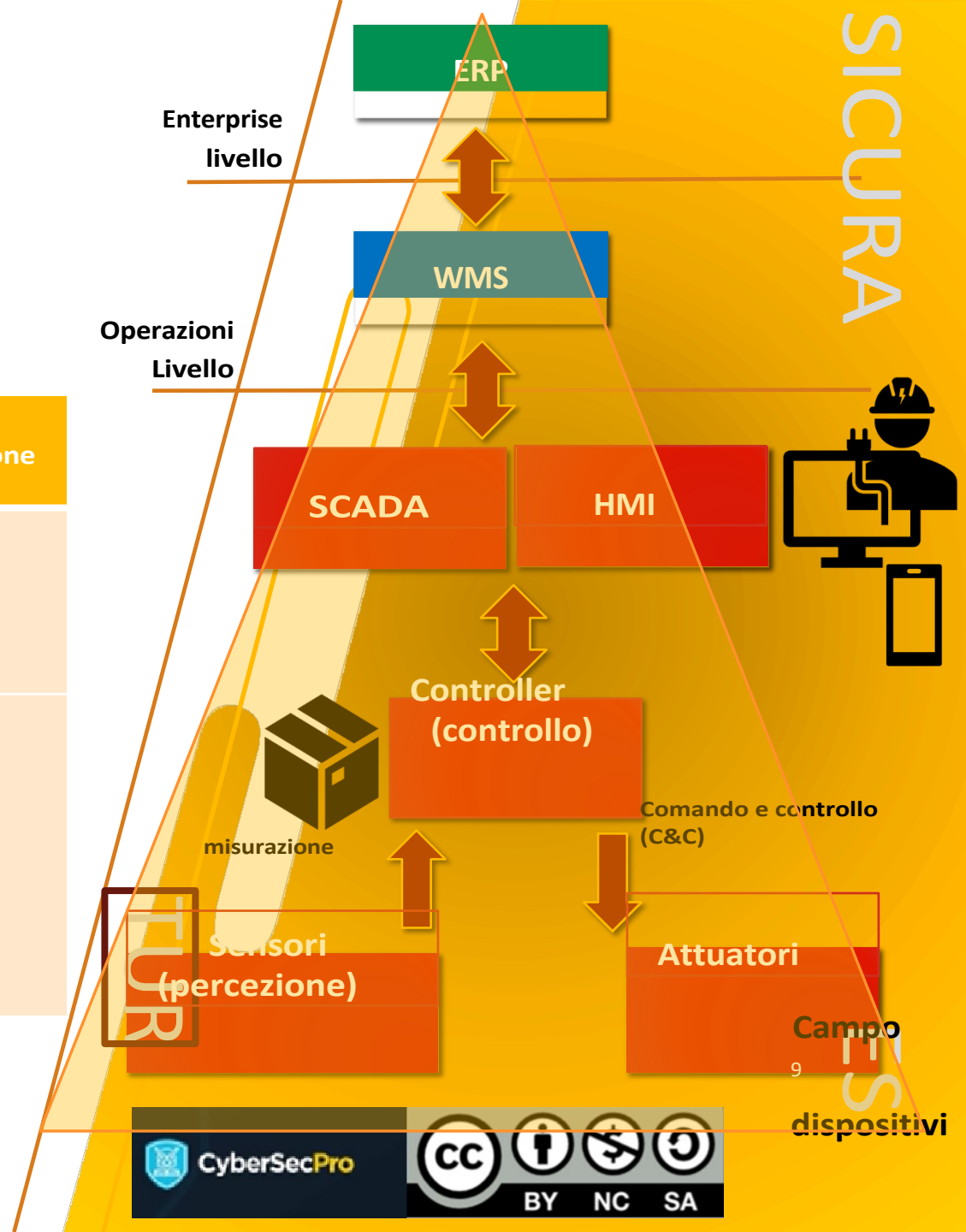
Livello funzionale	Componenti	Collegamenti di comunicazione
Livello aziendale (ERP)	Server ERP	Ethernet, wireless
Livello operativo (WMS)	Server WMS	Ethernet, wireless
Livello di controllo	Server SCADA, HMI, controller (PLC/RTU)	Ethernet, wireless
	Dispositivi di campo (sensori, attuatori)	Ethernet, comunicazione seriale, wireless



Reti principali nei sistemi energetici

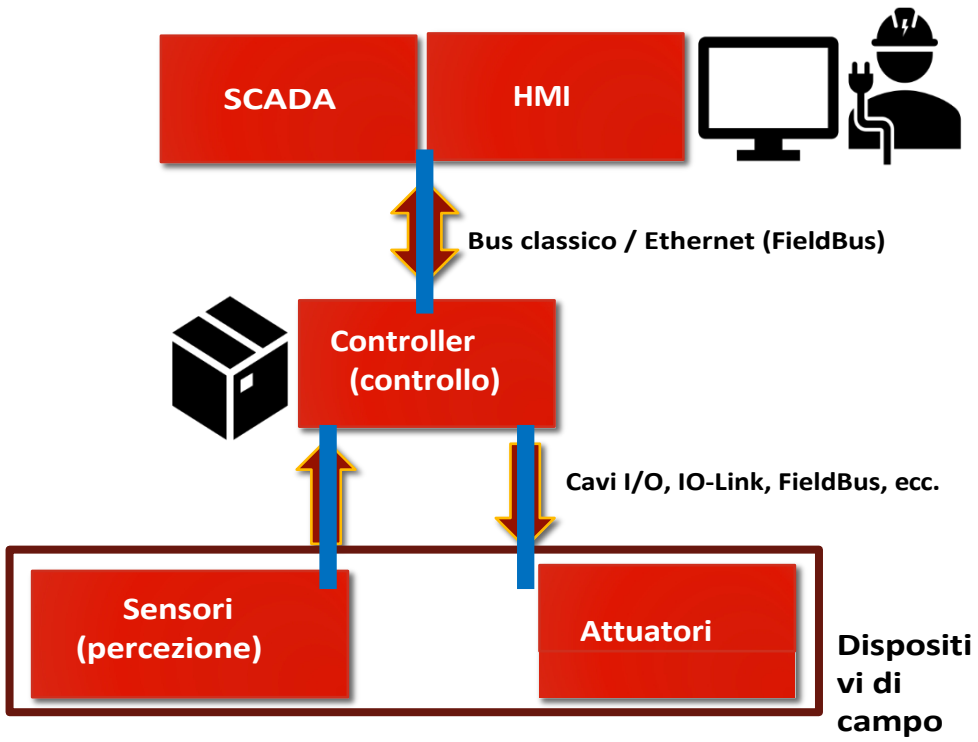
- Questa gerarchia operativa è composta da una serie di livelli funzionali:

Livello funzionale	Componenti	Collegamenti di comunicazione	Protocolli di comunicazione
Livello aziendale (ERP)	Server ERP	Ethernet, wireless	OPC-UA, Woopsa, MQTT, CoAP, AMQP,…
Livello operativo (WMS)	Server WMS	Ethernet, wireless	
Livello di controllo	Server SCADA, HMI, controllori (PLC/RTU)	Ethernet, wireless	OPC-UA, DNP3, Modbus RTU, ModbusTCP, EthernetIP, EthernetCAT, WirelessHART, ISA100.11a, IO-Link…
	Dispositivi di campo (sensori, attuatori)	Ethernet, comunicazione seriale, wireless	



Alcuni protocolli e caratteristiche di comunicazione

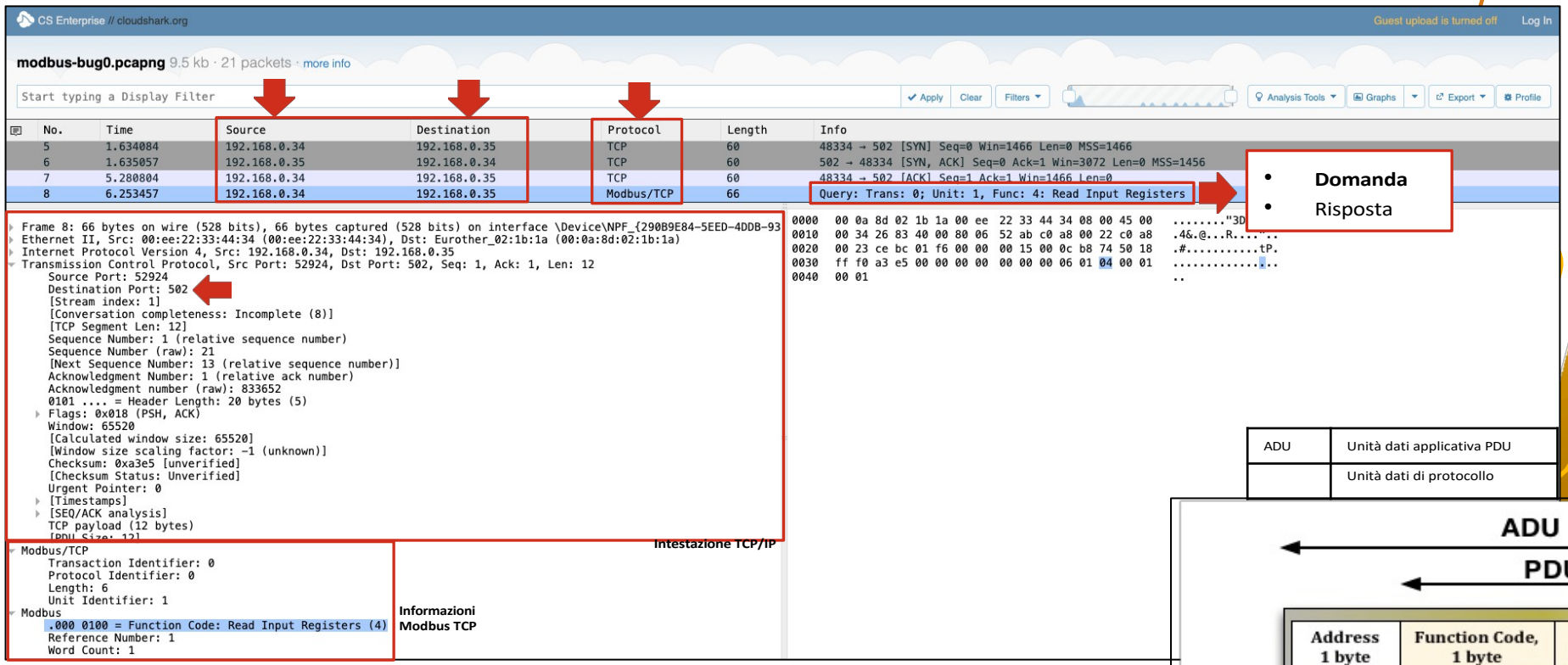
- **I protocolli del livello di controllo** sono composti da un insieme di dispositivi CPS collegati Peer-to-Peer (P2P) o tramite un bus di comunicazione, seguendo **connessioni master-slave**, dove il master riceve informazioni dallo slave a intervalli regolari



Alcuni protocolli e caratteristiche di comunicazione

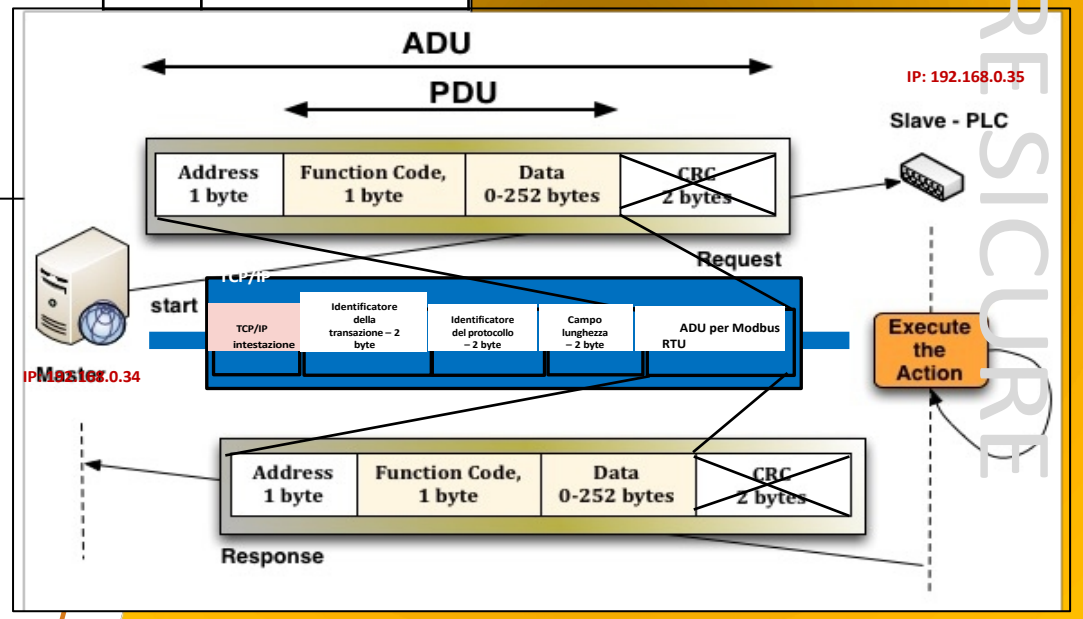
- Esiste una notevole varietà di **protocolli del livello di controllo**, sia open source che proprietari.

Alcuni protocolli	Comunicazione	Caratteristiche
IO-Link	• Connessione P2P	• Controller e dispositivi di campo • Gestione di stati e unità, con **diagnosi**, configurazione delle interfacce e gestione degli eventi
Modbus RTU	• Master/slave • Comunicazione seriale	• Controllori e dispositivi di campo • Utilizza la codifica binaria e aggiunge il controllo **CRC (Cyclic Redundancy Check)**
Modbus ASCII	• Master/slave • Comunicazione seriale.	• Controller e dispositivi di campo • Fornisce gli stessi obiettivi di Modbus RTU, ma applica caratteri ASCII per la comunicazione
Modbus TCP	• Master/slave • Comunicazione TCP/IP.	• Incapsula Modbus RTU su TCP/IP • **Non fornisce meccanismi di riservatezza e autenticazione** e verifica solo determinate parti dei pacchetti • **Non dispone di meccanismi anti-replay** per controllare gli attacchi DoS • Non include CRC perché è incluso dai livelli TCP/IP

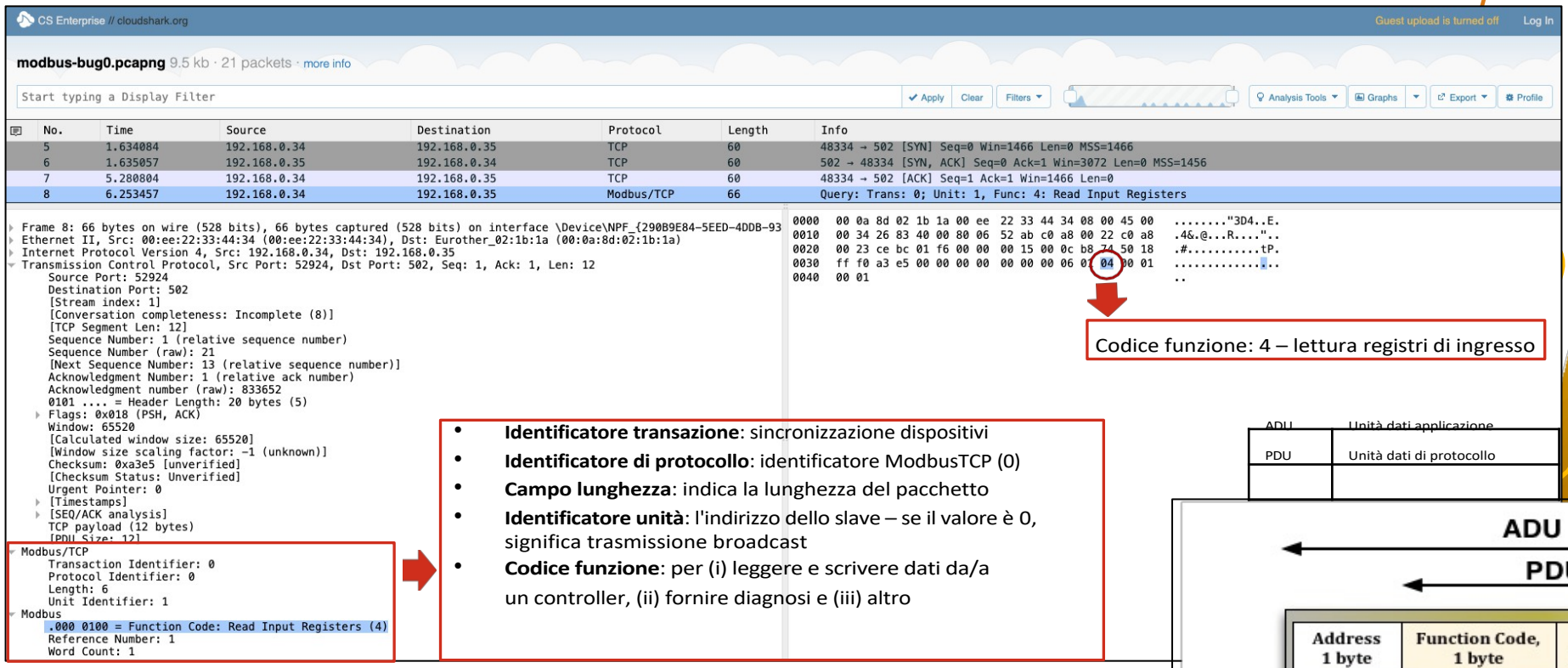


- **ModbusTCP**
  - 1 master può connettersi a 247 slave con ID univoci
  - I client e i server ascoltano e ricevono dati tramite la porta 502
  - I pacchetti Modbus RTU sono di 256 byte: 1 byte per l'indirizzo, 1 byte per il codice funzione, 0-252 byte per i dati e 2 byte per il CRC
  - Tuttavia, l'ADU ModbusTCP aggiunge l'MBAP (Modbus App. Protocol) con 7 byte: 1 byte per l'identificatore della transazione, 2 byte per l'identificatore del protocollo, 2 byte per il campo lunghezza e 1 byte per l'indirizzo (l'identificatore dell'unità == indirizzo di 1 byte in PDU)

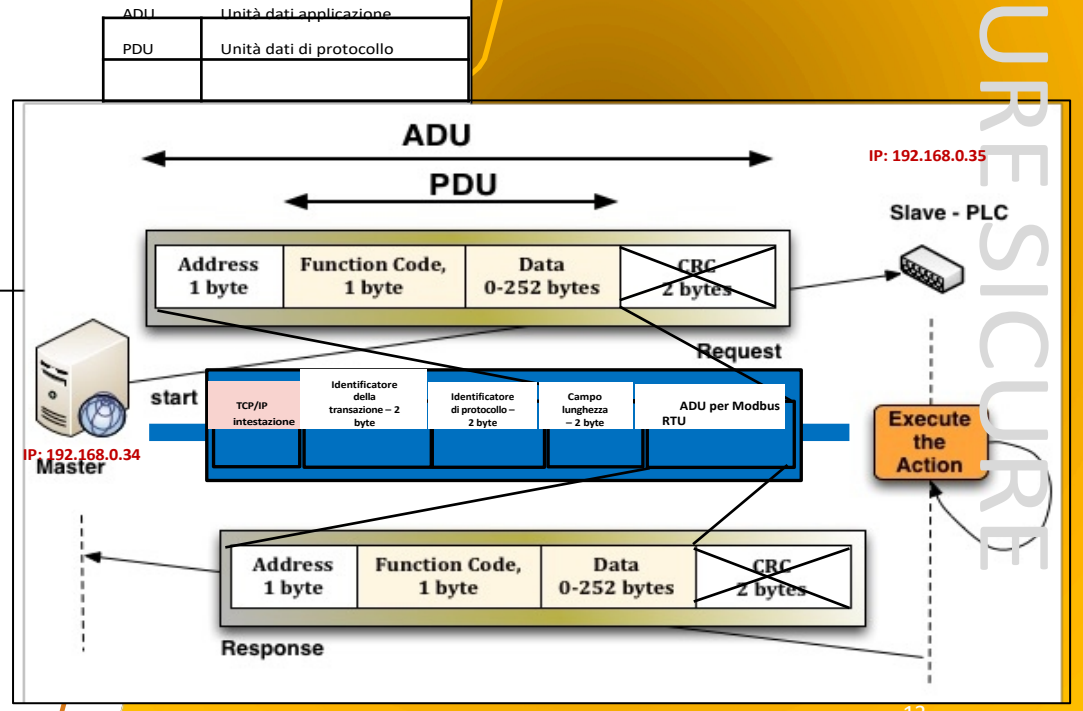
ADU	Unità dati applicativa PDU
	Unità dati di protocollo



Fonte della figura: CloudShark.org – modbus-bug0.pcapng URL:
https://www.cloudshark.org/captures/4b8f9f3579b3



- **Identificatore transazione**: sincronizzazione dispositivi
- **Identificatore di protocollo**: identificatore ModbusTCP (0)
- **Campo lunghezza**: indica la lunghezza del pacchetto
- **Identificatore unità**: l'indirizzo dello slave – se il valore è 0, significa trasmissione broadcast
- **Codice funzione**: per (i) leggere e scrivere dati da/a un controller, (ii) fornire diagnosi e (iii) altro



ModbusTCP

- 1 master può connettersi a 247 slave con ID univoci
- I client e i server ascoltano e ricevono dati tramite la porta 502
- I pacchetti Modbus RTU sono di 256 byte: 1 byte per l'indirizzo, 1 byte per il codice funzione, 0-252 byte per i dati e 2 byte per il CRC
- Tuttavia, l'ADU ModbusTCP aggiunge l'MBAP (Modbus App. Protocol) con 7 byte: 1 byte per l'identificatore della transazione, 2 byte per l'identificatore del protocollo, 2 byte per il campo lunghezza e 1 byte per l'indirizzo (l'identificatore dell'unità == indirizzo di 1 byte in PDU)

Fonte della figura: CloudShark.org – modbus-bug0.pcapng URL: https://www.cloudshark.org/captures/4b8f9f3579b3

Alcuni protocolli e caratteristiche di comunicazione

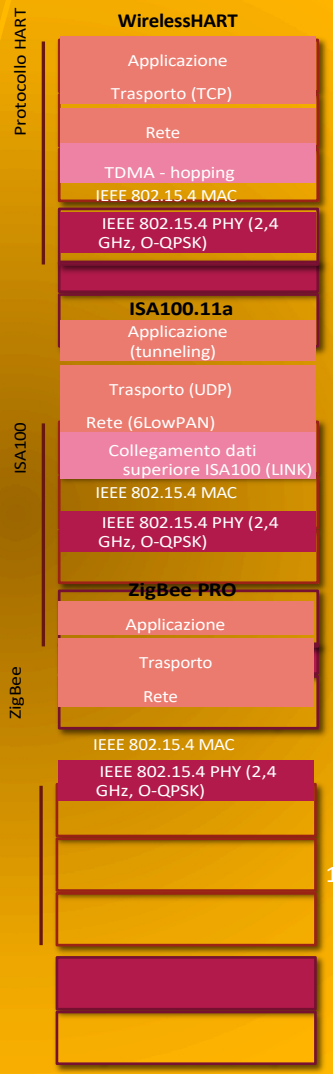
- Esiste una notevole varietà di **protocolli a livello di controllo**, sia open source che proprietari

Alcuni protocolli	Comunicazione	Caratteristiche
PROFIBUS	• Master/slave • Comunicazione basata su token in bus multipunto	• Offre molteplici servizi di controllo: PROFIsafe con **meccanismi di integrità** a supporto alla sicurezza operativa e PROFIdrive per **l'interazione basata sulla posizione** con i sistemi
PROFINET	• Funziona su Ethernet e TCP/IP	• Offre molteplici servizi di controllo: **diagnosi, allarmi,** configurazione, manutenzione e sincronizzazione • Estende i profili PROFIBUS per aggiungere funzionalità extra, in modo che una rete PROFINET possa controllare una rete PROFIBUS tramite interfacce PROFINET IO o un proxy
OPC-UA (OPC Unified Architecture)	• Comunicazione basata su oggetti, in cui ogni dispositivo è incapsulato in un oggetto	• Utilizza la codifica dei dati basata su XML-RPC (XML su HTTP) e si basa su due protocolli: protocollo binario basato su TCP/IP per prestazioni in tempo reale e protocollo basato su SOAP per gestire la rete tramite servizi Web • Offre servizi e rilevamento dei dispositivi, scambio di dati, **gestione degli eventi e avvisi**
CIP (Common Industrial Protocol)	• Comunicazione basata su oggetti, in cui ogni dispositivo è incapsulato in un oggetto • Ethernet/IP	• Offre molteplici servizi: controllo in tempo reale, sicurezza operativa, controllo della potenza, sincronizzazione e prioritizzazione, **autenticazione tramite TLS/DTLS in Ethernet/IP, controllo degli accessi, integrità e riservatezza**, ecc.
HART (Highway Addressable Remote Transducer)	• Connessione P2P e bus multipunto	• Controller e dispositivi di campo basati su comunicazioni analogiche • Scambio di dati (variabili, stati, parametri, dati, unità, configurazione)
HART/IP	• Funziona su HART Ethernet e TCP/IP per incapsulare i pacchetti HART	• Consente l'integrazione di una rete wirelessHART in una rete HART

Alcuni protocolli di comunicazione e caratteristiche

- Esiste una notevole varietà di **protocolli a livello di controllo**, sia open source che proprietari

Alcuni protocolli	Comunicazione	Caratteristiche
WirelessHART	• Comunicazioni P2P e reti mesh • Comunicazioni wireless basate sullo standard IEEE **802.15.4** (reti personali wireless a bassa velocità (LR-WPAN)) • Comunicazioni orientate ai comandi basate su HART (TCP)	• Controller/gateway e dispositivi di campo • Offre servizi per metodi **di salto di frequenza e blacklisting, crittografia e autenticazione**
ISA100.11a	• Comunicazione P2P e reti mesh • Comunicazione wireless basata su IEEE **802.15.4** (LR-WPAN) • Comunicazioni orientate agli oggetti sotto UDP • Compatibilità con 6LowPAN	• Controller/gateway e dispositivi di campo • Offre servizi per metodi **di salto di frequenza e blacklisting, crittografia e autenticazione**
ZigBee	• Comunicazione P2P e reti mesh • Comunicazioni wireless basate su IEEE **802.15.4** (LR-WPAN)	• Controller/gateway e dispositivi di campo • Offre servizi per **schemi di indirizzamento (stocastico, di gruppo), agilità di frequenza, crittografia e autenticazione**
ETC.	ETC.	ETC.

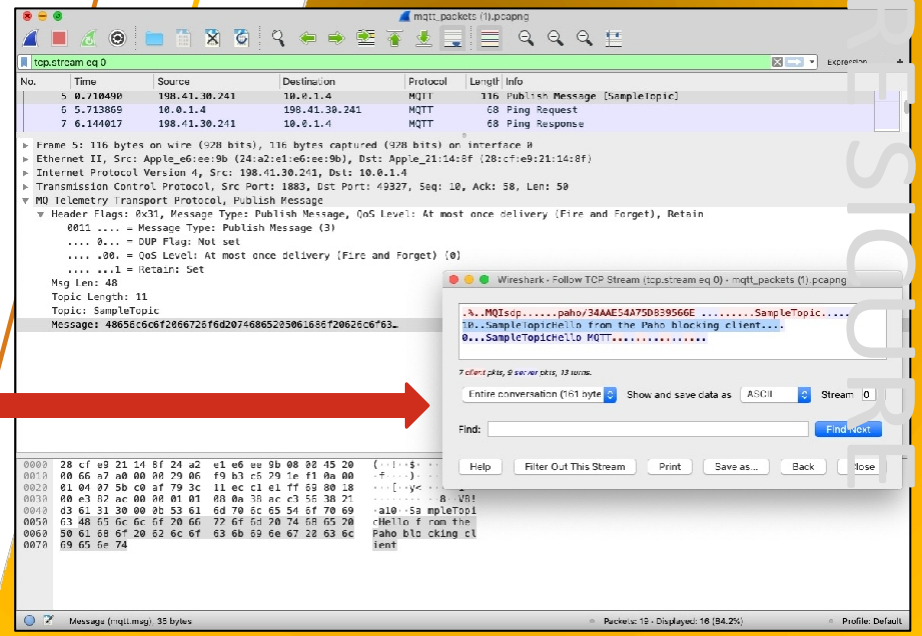


Alcuni protocolli e caratteristiche di comunicazione

- Esiste inoltre una notevole varietà di **protocolli a livello aziendale e operativo**, che funzionano su diverse infrastrutture di comunicazione
  - Architetture basate su cloud ed edge
  - Architetture basate su RESTful/REST come CoAP
  - Reti basate su publish/subscribe come MQTT o AMQP

Alcuni protocolli	Caratteristiche
CoAP (Constrained Application Protocol)	• Funziona su UDP, quindi **dipende da DTLS**
MQTT (Message Queue Telemetry Transport)	• Funziona su TCP basandosi su header leggeri per ridurre il consumo energetico e la larghezza di banda • **L'autenticazione** è gestita dai broker e tramite nome utente/password • **Non fornisce crittografia, quindi dipende da TLS**
AMQP (Queuing Protocol Advanced Message)	• Funziona su TCP e **dipende da TLS** per la sicurezza • Richiede elaborazione e memoria per gestire più code (probabilmente con informazioni duplicate), quindi non è consigliato per dispositivi con limitazioni

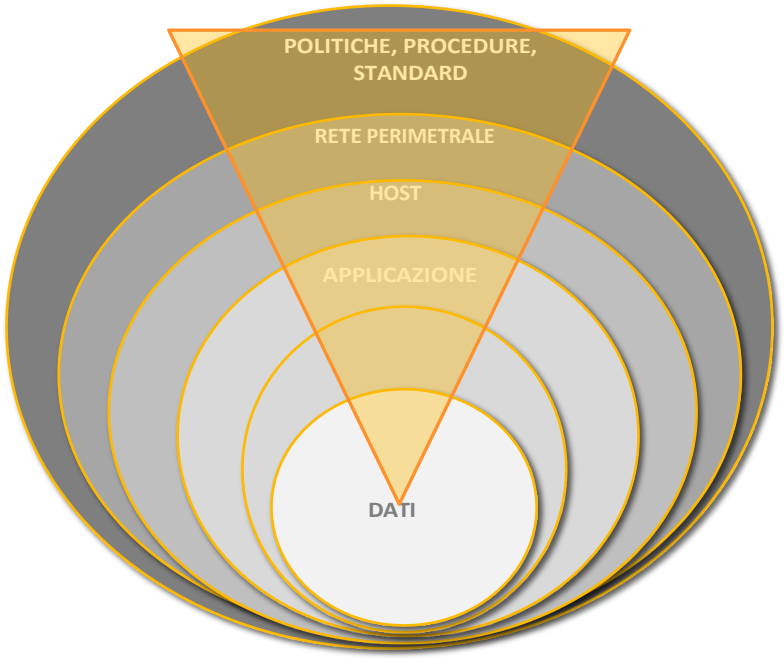
TLS	Transport Layer Security, garantisce la sicurezza sul livello di trasporto e su TCP
DTLS	Datagram Transport Layer Security, offre la stessa sicurezza di TLS ma su UDP



Fonte dell'immagine: Pradeesi, MQTT-Wireshark-Capture
URL: https://github.com/pradeesi/MQTT-Wireshark-Capture/blob/master/mqtt_packets.pcapng

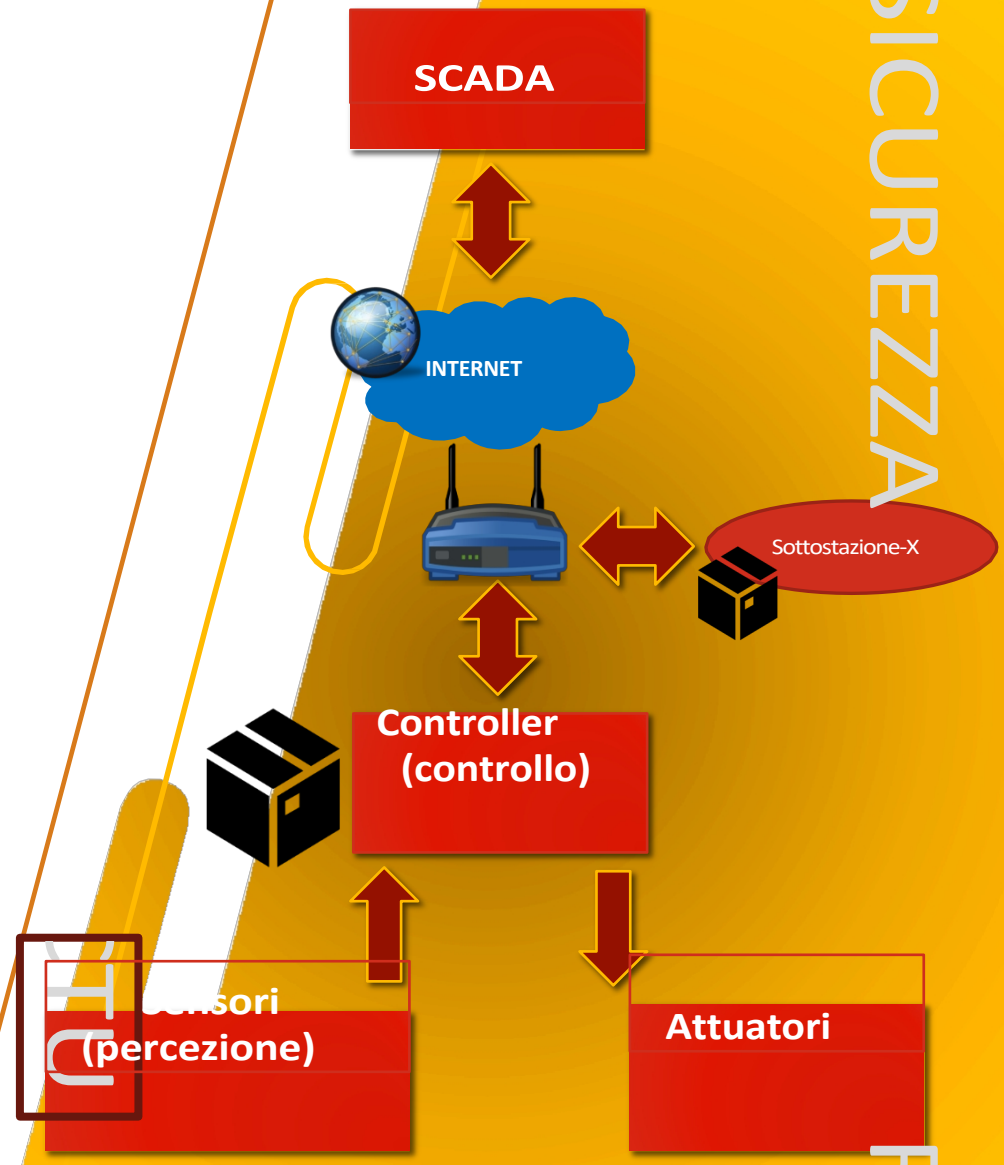
Architetture sicure in base ai principi di sicurezza

- Esistono quindi molti protocolli che aggiungono misure di sicurezza o che si affidano in larga misura a meccanismi esterni, come TLS/DTLS, per garantire la riservatezza, l'autenticazione e l'integrità
  - Ma anche in questo caso, è necessario prendere in considerazione altre misure di sicurezza seguendo il buon principio della "***difesa in profondità***"



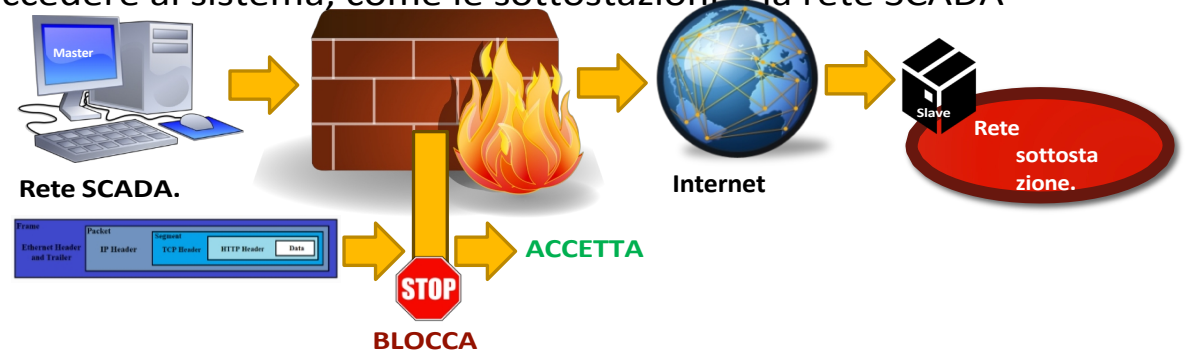
Architetture sicure:
A livello di perimetro di rete

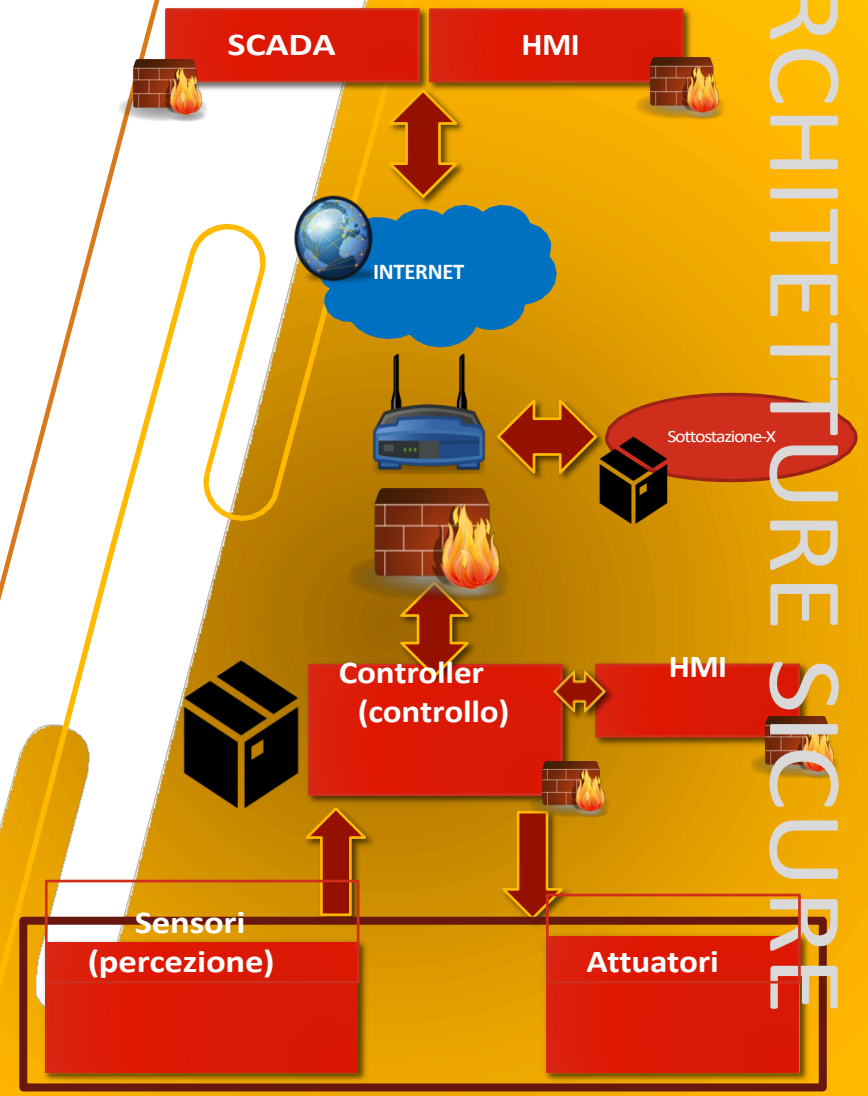
- **Router**:
  - Dispositivo in grado di filtrare il traffico di rete e determinare il percorso successivo di un pacchetto
  - Questa capacità di filtraggio consente al sistema di stabilire politiche di connessione e accesso, scartando i pacchetti in entrata/uscita verso una rete



Architetture sicure:
A livello di perimetro di rete

- **Router**:
  - Dispositivo in grado di filtrare il traffico di rete e determinare il percorso successivo di un pacchetto
  - Questa capacità di filtraggio consente al sistema di stabilire politiche di connessione e accesso, scartando i pacchetti in entrata/uscita verso una rete
- **Firewall**:
  - Componente HW/SW in grado di filtrare i pacchetti in entrata/uscita attraverso una serie di regole firewall.
  - Queste regole stabiliscono quale traffico di rete può (e non può) accedere al sistema, come le sottostazioni o la rete SCADA

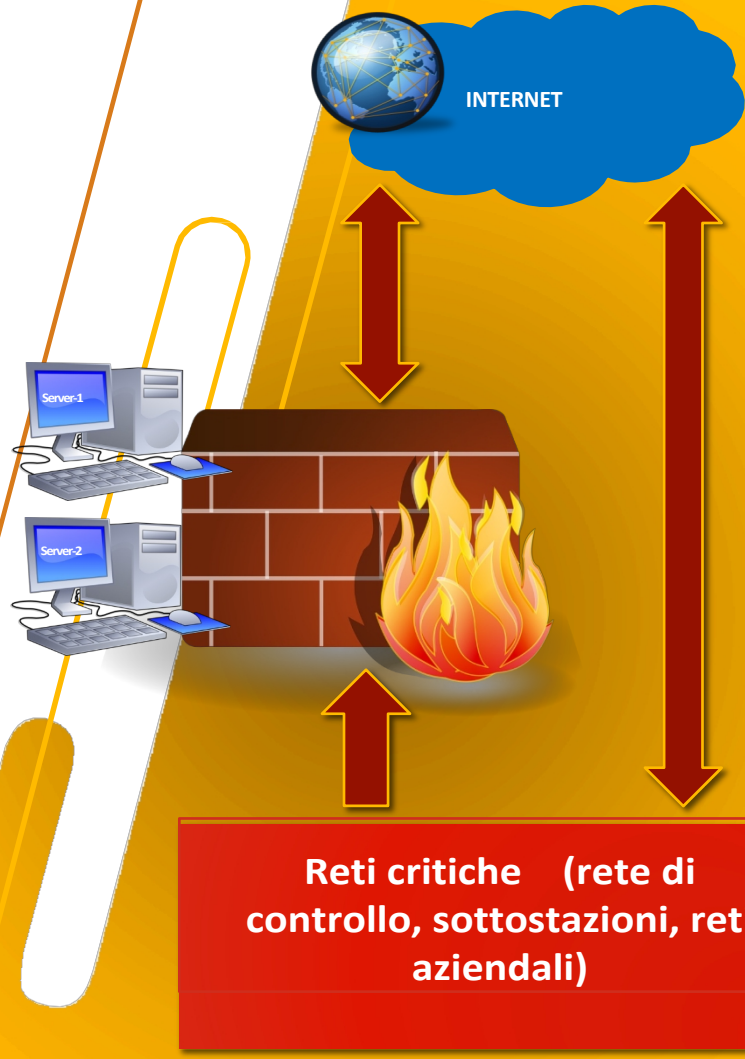




ARCHITETTURE SICURE

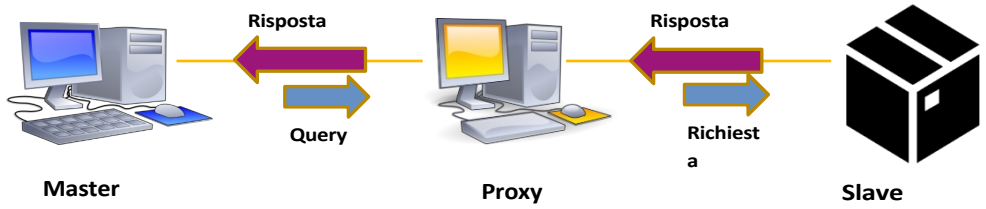
Architetture sicure:
A livello di perimetro di rete

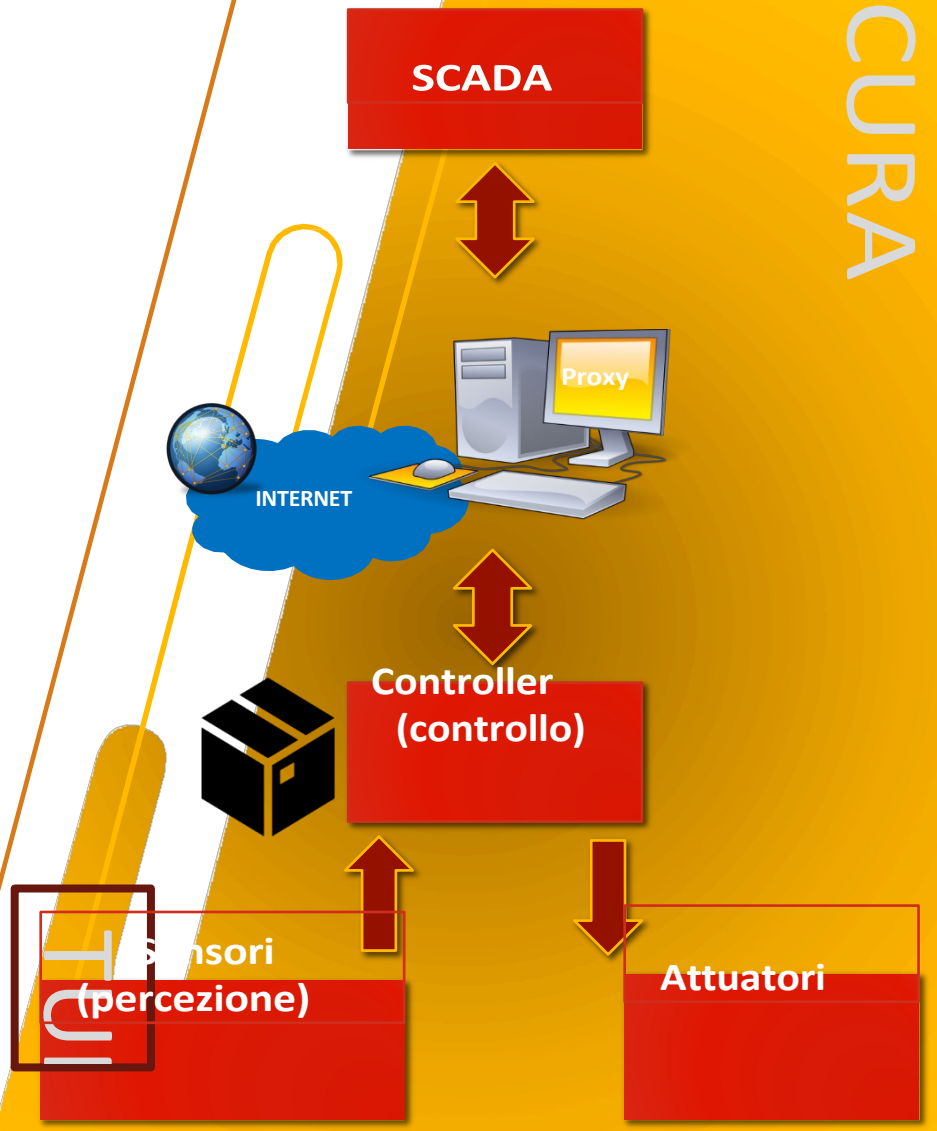
- **Router**:
  - Dispositivo in grado di filtrare il traffico di rete e determinare il percorso successivo di un pacchetto.
  - Questa capacità di filtraggio consente al sistema di stabilire politiche di connessione e accesso, scartando i pacchetti in entrata/uscita verso una rete
- **Firewall**:
  - Componente HW/SW in grado di filtrare i pacchetti in entrata/uscita attraverso una serie di regole firewall
  - Queste regole stabiliscono quale traffico di rete può (e non può) accedere al sistema, come le sottostazioni o la rete SCADA
- **DMZ (zona demilitarizzata)**:
  - Crea sottoreti composte da server che devono essere interrogati da reti esterne come Internet, *utili per le reti aziendali*
  - Pertanto, le DMZ si basano su regole firewall che isolano la rete di sicurezza dalle altre reti



Architetture sicure:
A livello di perimetro di rete

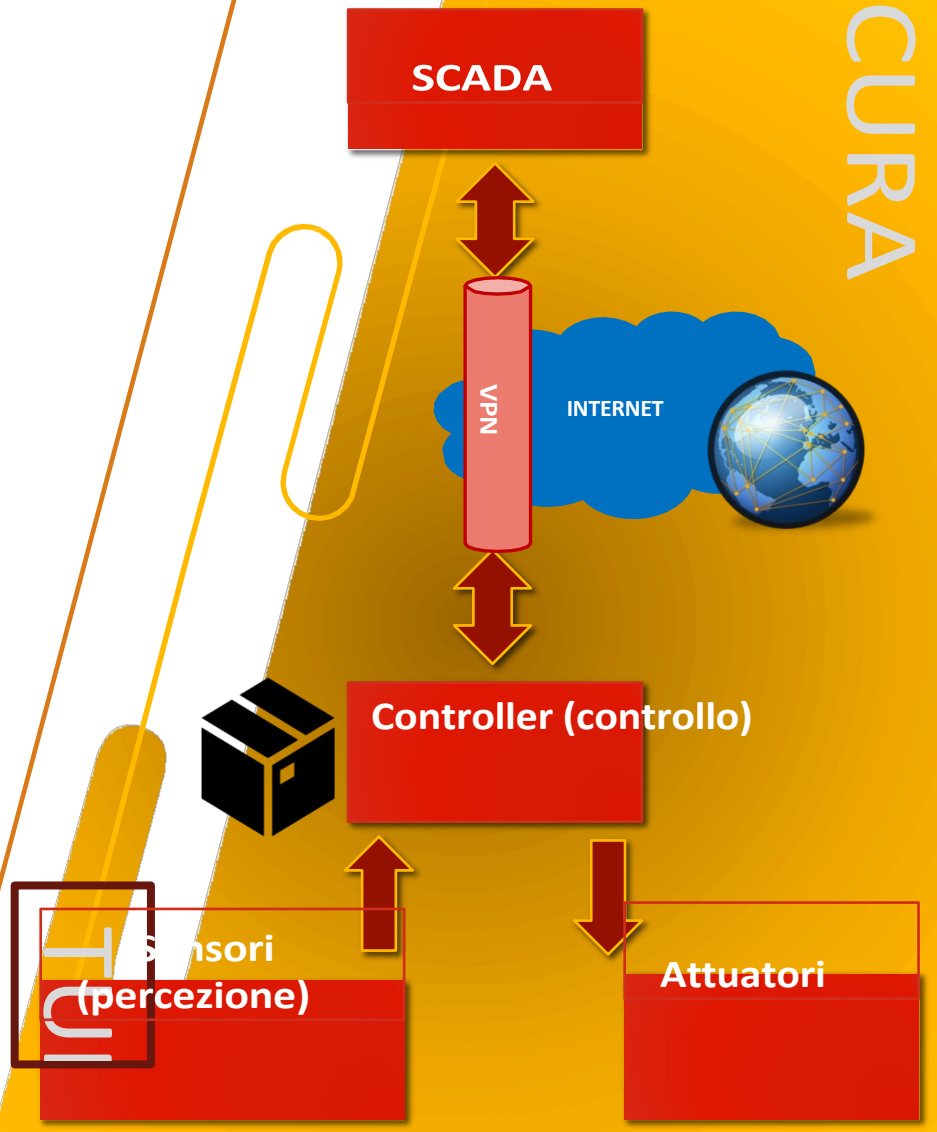
- **Proxy**:
  - Dispositivo intermedio tra un nodo client e un server (ad esempio tra un master e uno slave), in grado di aggiungere ulteriori misure di sicurezza
    - Ad esempio, nascondendo gli IP dei nodi distribuiti in reti vulnerabili, come le sottostazioni
  - Questo processo di occultamento consiste nel sostituire gli IP dei nodi vulnerabili con l'IP del proxy:
    - Tutto il traffico in entrata verso un IP del controller è protetto attraverso Internet utilizzando l'IP del proxy nei pacchetti
    - Tutto il traffico in uscita da un IP del controller verso il master è protetto sostituendo questo IP con l'IP del proxy
  - Questo tipo di protezione evita successivamente attacchi *di analisi passiva del traffico*





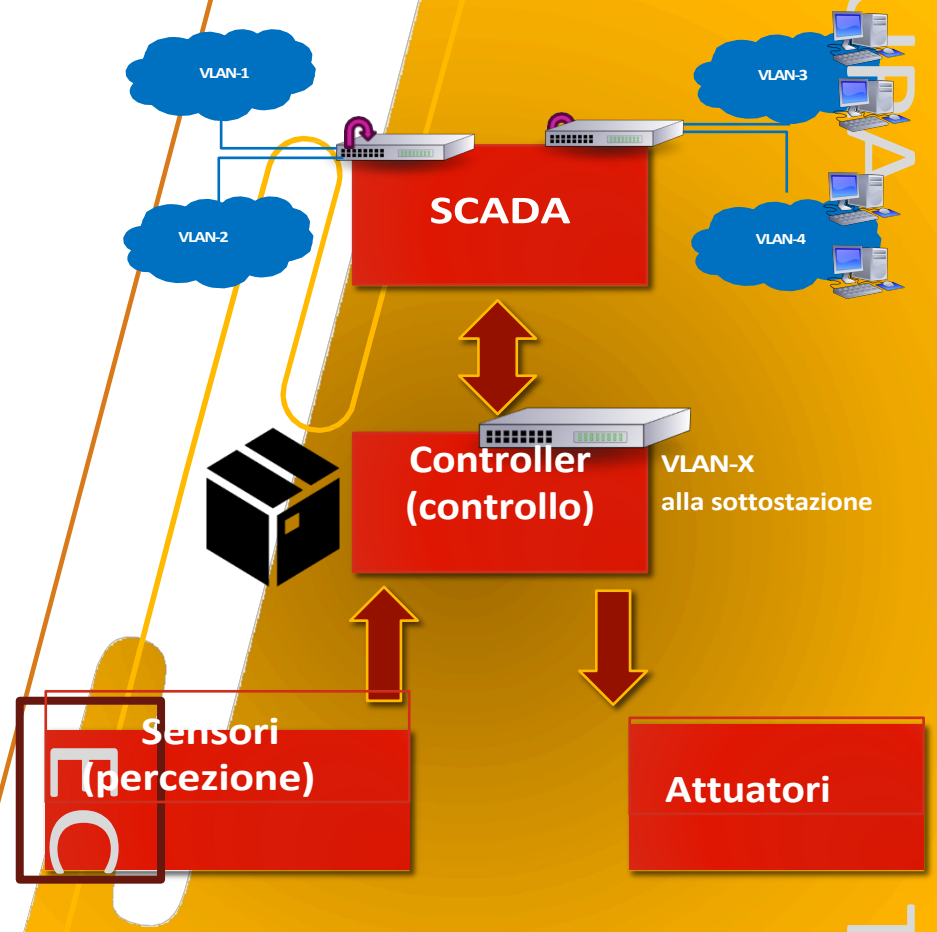
Architetture sicure:
A livello di perimetro di rete

- **Rete privata virtuale (VPN)**:
  - Corrisponde a una connessione P2P, i cui canali di comunicazione sono protetti dalla configurazione di misure di sicurezza avanzate (relative a riservatezza, integrità e autenticazione).
  - Queste VPN possono essere configurate tra diversi dispositivi (di controllo), sia tra master e slave, tra slave, tra router, ecc.
  - Esistono molti tipi di VPN supportati da diversi protocolli di sicurezza, che saranno descritti in dettaglio nelle prossime sessioni di questo corso



Architetture sicure:
A livello di perimetro di rete

- **Rete privata virtuale (VPN)**:
  - Corrisponde a una connessione P2P, i cui canali di comunicazione sono protetti dalla configurazione di solide misure di sicurezza (relative a riservatezza, integrità e autenticazione).
  - Queste VPN possono essere configurate tra diversi dispositivi (di controllo), sia tra master e slave, tra slave, tra router, ecc.
  - Esistono molti tipi di VPN supportati da diversi protocolli di sicurezza, che saranno descritti in dettaglio nelle prossime sessioni di questo corso
- **LAN virtuale (VLAN)**:
  - Corrisponde a una rete locale (LAN) "virtuale" le cui connessioni sono stabilite logicamente nello switch/bridge
  - Cioè, una porta fisica dello switch/bridge è riservata a più connessioni logiche, indipendentemente dalla posizione degli utenti
  - Questa rete "virtuale" consente:
    - La connessione locale di operatori umani, amministratori o ingegneri alle reti e aumenta le capacità di connessione
    - La mobilità di questi operatori in tutto o in parte del sistema
    - Isolamento delle sottoreti vulnerabili rispetto al denial of service, più specificatamente agli attacchi basati sulla trasmissione

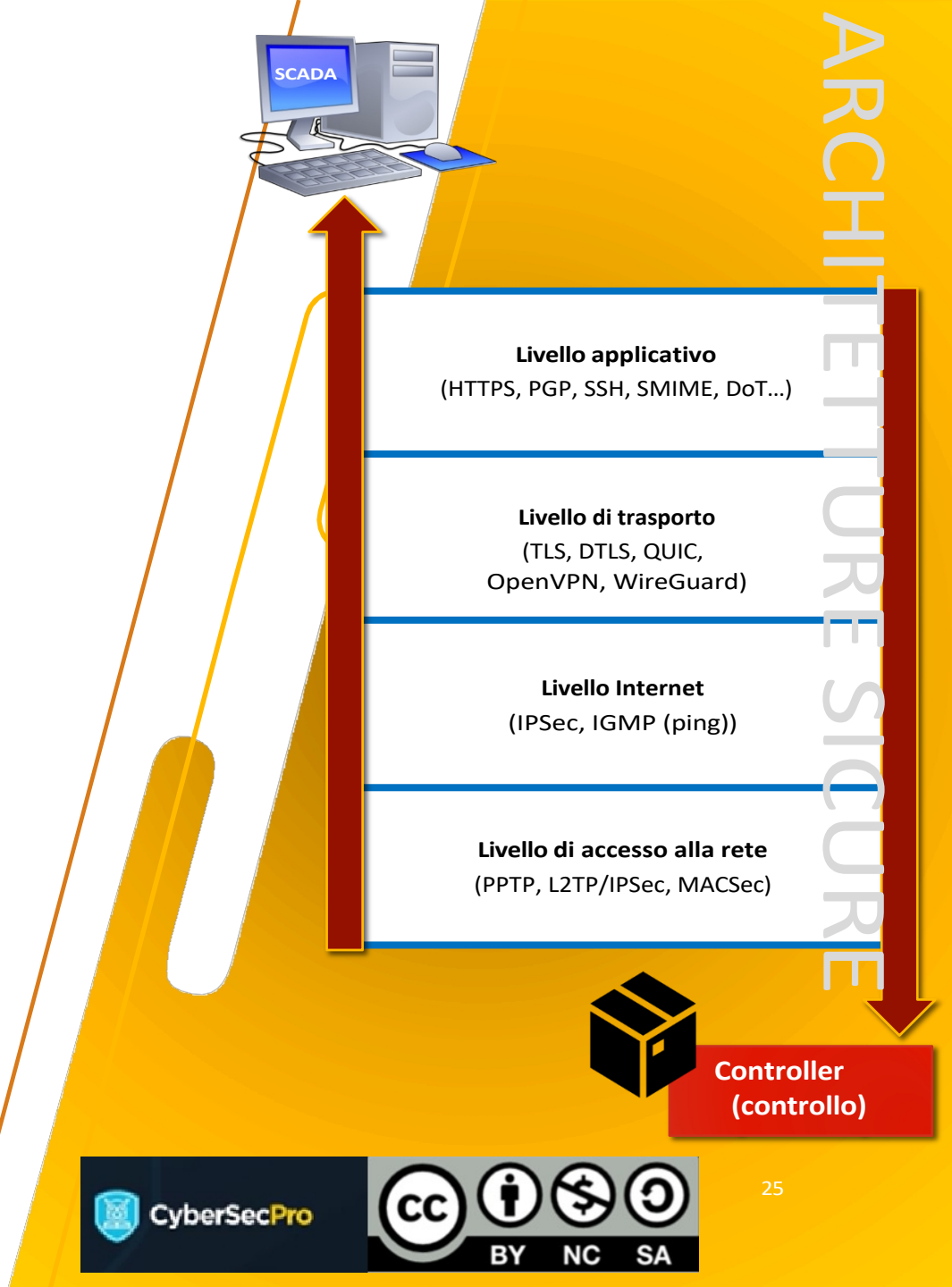


Architetture sicure:
A livello di perimetro di rete

- **Sistema di rilevamento delle intrusioni (IDS)**:
  - Sistema in grado di raccogliere, analizzare e segnalare attività anomale o dannose
  - Questa capacità di rilevamento può basarsi su una serie di modelli o regole per dedurre comportamenti anomali, oppure su modelli avanzati di apprendimento automatico
  - Esistono inoltre diversi tipi di IDS, a livello di rete e di host, che descriveremo in dettaglio nel corso di questo corso
- **Sistema di prevenzione delle intrusioni (IPS)**:
  - È un sistema equivalente a un IDS, ma con la capacità di fornire le stesse azioni di rilevamento aggiungendo capacità di risposta
  - Pertanto, un IPS è in grado di rilevare e rispondere a eventi anomali

Architetture sicure:
A livello di servizi di rete

- Attualmente, lo stack TCP/IP si basa su una serie di protocolli specifici, alcuni sviluppati originariamente per lo stack, altri progettati in base alle esigenze, quali:
  - *Transport Layer Security (TLS)*
  - *Internet Protocol Security (IPSec)*
  - *Datagram Transport Layer Security (DTLS)*
  - *Quick UDP Internet Connections (QUICK)*
  - *Protocollo di trasferimento ipertestuale sicuro (HTTPS)*
  - *Secure Shell (SSH)*
  - *Sistema dei nomi di dominio (DNS) su TLS (DoT)*
  - *DNS su HTTPS (DoH)*
  - *Pretty Good Privacy (PGP)*
  - *Estensioni di posta elettronica sicure e multiuso (SMIME)*
  - *…*
- Tutti questi servizi sono sviluppati attraverso lo stack, fornendo diverse misure di sicurezza



Architetture sicure:
A livello di standard

- Molte di queste misure sono prese in considerazione dagli attuali standard di sicurezza per i sistemi di alimentazione, quali:
  - **IEC** 62351 relativa alla "*Gestione dei sistemi di alimentazione e scambio di informazioni associate - Sicurezza dei dati e delle comunicazioni*"
    - La norma copre vari aspetti relativi alla protezione delle reti energetiche distribuite, tra cui: sicurezza per IEC 60870 (per apparecchiature e sistemi di telecontrollo), sicurezza per 61850 (nelle sottostazioni), sicurezza dei dati e delle comunicazioni, controllo degli accessi basato sui ruoli nelle sottostazioni, ecc.
    - Le misure vanno dall'uso tipico di soluzioni di crittografia e autenticazione all'applicazione di protocolli di sicurezza (TLS), comunicazione wireless e difesa perimetrale (VLAN e IDS).
  - **ISA/IEC 62443** sulla "*Sicurezza per i sistemi di automazione e controllo industriale*"
    - La norma stabilisce i requisiti di sicurezza, le condizioni e le raccomandazioni necessarie per fornire garanzie di protezione.
    - Anche queste protezioni sono molto varie e vanno dall'uso di soluzioni di crittografia e autenticazione alla sicurezza wireless, alla segmentazione della rete, all'accesso e alla gestione delle risorse, ai backup, alla responsabilità, ecc.

Considerazioni finali

- Abbiamo visto che le infrastrutture di controllo seguono tipicamente una struttura gerarchica, basata su più protocolli di comunicazione industriali
  - Molti di questi protocolli, sia proprietari che open source, non integrano necessariamente misure di sicurezza efficaci
  - È quindi necessario rafforzare la sicurezza seguendo i principi della "***difesa in profondità***"
- Questa difesa deve essere attuata a diversi livelli per ottenere il concetto di "*difesa in profondità*":
  - A livello di perimetro di rete
  - A livello dei servizi di rete
  - A livello normativo, tenendo conto degli attuali standard di sicurezza nelle reti elettriche e nelle sottostazioni

Riferimenti e fonti

1. CloudShark.org – modbus-bug0.pcapng, 2024
   URL: https://www.cloudshark.org/captures/4b8f9f3579b3
2. Vanimpe, "Introduzione al traffico Modbus TCP", 2015 URL: https://www.cloudshark.org/captures/4b8f9f3579b3
3. DeepL Translator per la revisione: https://www.deepl.com/translator

Connettiti con CyberSecPro: come registrarsi e altre informazioni pratiche

1. Sito web: www.cybersecpro-project.eu
2. X (Twitter): https://twitter.com/CyberSecPro_eu
3. LinkedIn: https://www.linkedin.com/company/cybersecpro-euproject/

Grazie

Per qualsiasi domanda, non esitate a contattare:

- Antonio Muñoz
  Professore associato
  Università di Malaga
  anto@uma.es